รีวิว
จเร เลิศสุดวิชัย

# CPAV
# อัศวินผู้ต่อต้านไวรัสคอมพิวเตอร์

*CPAV วัคซีนช่วยป้องกันและ กำจัดไวรัสที่มีศักยภาพ การทำงานที่สูงสุด*

ไวรัสคอมพิวเตอร์เกิดขึ้นใหม่ตลอดเวลา แม้ว่าในขณะนั้นเราได้โปรแกรมปราบไวรัสรุ่นใหม่มาก็ตาม ซึ่งอาจจะมีความสามารถปราบไวรัสได้มากมายหลายตัว แต่ก็ไม่สามารถใช้กำจัดไวรัสตัวที่เรากำลังเผชิญอยู่ได้ ต้องรอคอยฟังข่าวและค้นหาซอฟต์แวร์หรือโปรแกรมปราบไวรัสรุ่นใหม่ ๆ มาใช้ ดังนั้นในปัจจุบันจะพบว่าซอฟต์แวร์กำจัดไวรัสที่ออกมาใหม่ ช่วงนี้มักจะเป็นชุดโปรแกรมที่ประกอบไปด้วยโปรแกรมสำหรับปราบหรือกำจัดไวรัสโดยตรง โปรแกรมสำหรับป้องกันยับยั้งการแพร่กระจายพร้อมทั้งปกป้องจุดที่ไวรัสจะเข้าจู่โจมหรือทำลาย

การพิจารณาเลือกซื้อซอฟต์แวร์ปราบไวรัส นอกจากจะต้องพิจารณาถึงจำนวนและชนิดของไวรัสที่โปรแกรมสามารถกำจัดได้แล้ว คุณสมบัติอีกประการหนึ่งที่จะต้องพิจารณาด้วยก็คือคุณสมบัติของการป้องกันการแพร่กระจายไวรัสและการป้องกันการเข้าทำลายของไวรัสเมื่อไวรัสเข้าสู่ระบบแล้ว เนื่องจากระบบไมโครคอมพิวเตอร์เป็นระบบเปิด (Open System) ซึ่งเป็นเหตุให้มีการพัฒนาโปรแกรมไวรัสที่มีความสามารถในการแพร่กระจายเข้าระบบได้ง่ายพร้อมทั้งความสามารถในการจู่โจมทำลายระบบตามจุดที่สำคัญ ๆ ของระบบ ดังนั้นในบทความนี้จะกล่าวถึงรายละเอียดของจุดหรือช่องทางที่ไวรัสคอมพิวเตอร์จะสามารถแพร่กระจายเข้าสู่ระบบได้ รวมทั้งการระมัดระวังจุดอ่อนต่าง ๆ ที่ไวรัสจะเข้าจู่โจม รายละเอียดเหล่านี้จะเป็นข้อมูลให้ผู้อ่านนำไปพิจารณาประกอบในการเลือกซื้อโปรแกรมป้องกันไวรัส พร้อมทั้งได้ทำการแนะนำชุดโปรแกรมปราบไวรัส CPAV (Central

Point Anti-Virus) ซึ่งเป็นชุดโปรแกรมปราบไวรัสชุดหนึ่งที่ท่านผู้อ่านควรมีเอาไว้ใช้งาน

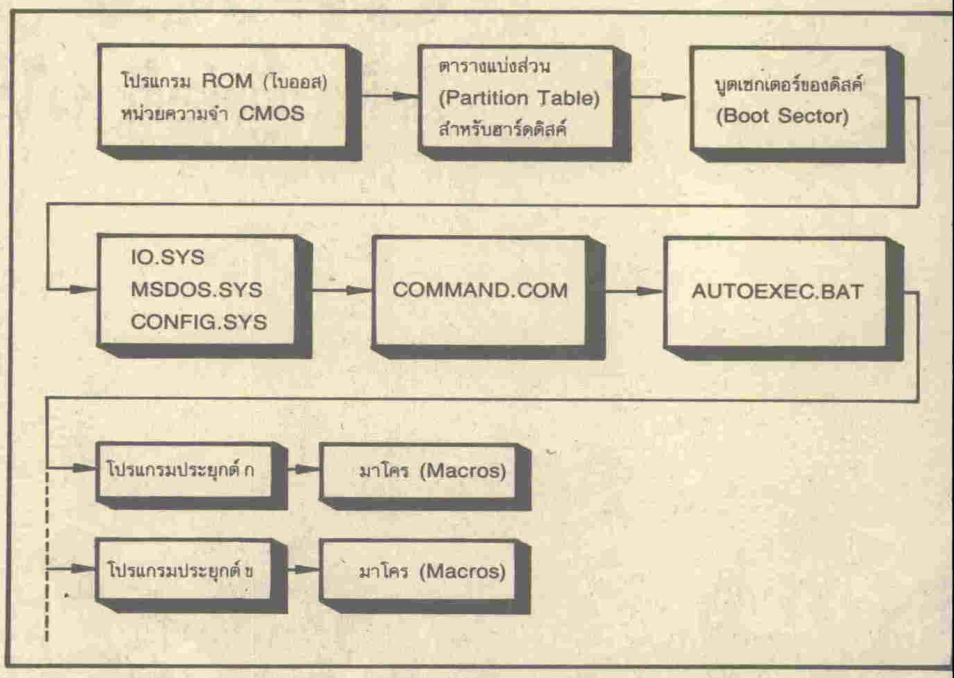
## จุดที่ไวรัสจะเข้าจู่โจม

หากพิจารณาการทำงานของไวรัสคอมพิวเตอร์ เราจะพบว่าพฤติกรรมที่สำคัญของไวรัสมีอยู่ 2 ประการด้วยกัน คือ พฤติกรรมการแพร่กระจายและการทำลายล้าง ซึ่งในพฤติกรรมการแพร่กระจายนั้นไวรัสจะเข้าแพร่กระจายหรือติดตั้งตัวเองในจุดเปิดต่าง ๆ ของเครื่อง เมื่อเข้าไปเกาะติดในจุดเหล่านั้นแล้วไวรัสจะสามารถถูกเรียกขึ้นมาทำงานและครอบครองระบบได้ ส่วนพฤติกรรมการทำลายล้างนั้นเมื่อไวรัสครอบครองระบบแล้วโดยส่วนใหญ่มักจะมีการทำลายระบบโดยเฉพาะส่วนสำคัญของการทำงานทั้งหมดก็คือข้อมูล ดังนั้นเป้าหมายของพฤติกรรมนี้คือ จุดอ่อนต่าง ๆ ในการเก็บข้อมูลของระบบซึ่งมักจะเป็นฮาร์ดดิสก์หรือฟลอปปี้ดิสก์ เป็นต้น

ดังนั้นจึงพอจะแยกเป้าหมายที่ไวรัสจะเข้าจู่โจมได้เป็น 2 ประเภทใหญ่ ๆ คือ เป้าหมายการแพร่กระจายและเป้าหมายการทำลายล้าง

## เป้าหมายการแพร่กระจาย

ไวรัสจะแพร่กระจายตัวเองเข้าไปในระบบ โดยจุดที่ไวรัสจะเกาะติดจะต้องเป็นจุดที่ไวรัสสามารถถูกเรียกขึ้นมาทำงานในระบบได้ ซึ่งเมื่อถูกเรียกขึ้นมาทำงานไวรัสก็จะเข้าครอบครองระบบได้อย่างเต็มที่ ดังนั้นเพื่อที่จะได้ทราบถึงจุดเปิดต่าง ๆ ของระบบที่อาจจะถูกไวรัสเข้าแพร่กระจายได้ จึงควรที่จะทราบถึงลำดับขั้นตอนการทำงานของเครื่องดังนี้




รูปที่ 1 แสดงขั้นตอนการทำงานของเครื่องตั้งแต่เปิดเครื่อง จนกระทั่งถึงโปรแกรมประยุกต์ที่นิยมใช้งาน

เมื่อเริ่มต้นเปิดเครื่อง (power on) หรือในขณะที่เปิดเครื่องแล้วกด Ctrl+Alt+Del เพื่อเข้าสู่ระบบปฏิบัติการ (DOS) จนกระทั่งสุดท้ายคือ โปรแกรมประยุกต์ (Application Program) ต่าง ๆ ที่นิยมใช้งานกัน เช่น ดีเบส โลตัส เป็นต้น ขั้นตอนต่าง ๆ แสดงเป็นไดอะแกรมดังรูปที่ 1 โดยรายละเอียดแต่ละขั้นตอนอธิบายได้ดังนี้

1. เมื่อเปิดเครื่องขึ้นมาใหม่ หรือเมื่อทำการวอร์มบูต (Ctrl+Alt+Del) เครื่องจะเริ่มทำงานขั้นแรกโดยโปรแกรมไบออสในหน่วยความจำรอมของเครื่อง ในการทำงานของโปรแกรมไบออสจะทดสอบอุปกรณ์ต่าง ๆ ที่ต่อพ่วงอยู่กับเครื่อง จากนั้นจึงจะทดสอบหาดิสค์ไดรฟ์ (ซึ่งอาจจะเป็นฮาร์ดดิสก์หรือฟลอปปี้ดิสค์) และอ่านเอาข้อมูลในเซกเตอร์แรกของดิสค์มาไว้ในหน่วยความจำแรม ข้อมูลดังกล่าวก็คือโปรแกรมสั้น ๆ ที่เราเรียกว่า Bootstrap สำหรับเรียกเอาระบบปฏิบัติการขึ้นมาทำงานอีกต่อหนึ่ง หลังจากโหลดหรืออ่านโปรแกรม Bootstrap มาที่หน่วยความจำแรมแล้ว เครื่องจะโอนการทำงานให้โปรแกรม Bootstrap ต่อไป แต่สำหรับดิสค์ที่ไม่มีโปรแกรม Bootstrap เครื่องก็จะแสดงข้อความว่า "Non-System Disk" (หรือข้อความอื่นที่บอกว่าดิสค์ดังกล่าวไม่มีโปรแกรมระบบ) และรอให้ผู้ใช้เปลี่ยนเอาแผ่นใหม่ที่มีโปรแกรมระบบมาใส่แทน

สำหรับเครื่องระดับ AT ระบบจะอ่านข้อมูลที่เก็บเอาไว้ในหน่วยความจำเล็ก ๆ คือ ซีมอส (CMOS) ซึ่งข้อมูลภายในหน่วยความจำนี้จะเป็นข้อมูลที่บ่งบอกถึงคุณสมบัติของเครื่องและชนิดของอุปกรณ์ที่ต่อพ่วงกับระบบ โดยข้อมูลดังกล่าวสามารถติดตั้งได้ด้วยโปรแกรมยูทิลิตี้ SETUP (หรือในเครื่องรุ่นใหม่ โปรแกรม SETUP จะถูกบรรจุ

เอาไว้ในไบออสเลย โดยสามารถเรียกขึ้นมาทำงานได้ด้วยการกดแป้นพิมพ์พิเศษ เช่น Ctrl+Alt+Esc)

2. ในกรณีที่มีฮาร์ดดิสค์อยู่ ข้อมูลในเซกเตอร์แรกที่ถูกอ่านขึ้นมาจะเป็นตารางแบ่งส่วน (Partition Table) ซึ่งเป็นข้อมูลที่บ่งบอกถึงการแบ่งส่วนของฮาร์ดดิสค์ที่มีขนาดใหญ่ออกเป็นส่วน ๆ ว่ามีการใช้งานอย่างไรบ้าง ซึ่งในข้อมูลตารางแบ่งส่วนก็มีโปรแกรมสั้น ๆ ที่จะทำการอ่านเอาโปรแกรม Bootstrap ตัวจริงที่อยู่ในส่วนของฮาร์ดดิสค์ ซึ่งมีระบบปฏิบัติการดอสอยู่ต่อไป

3. ในกรณีของฟลอปปี้ดิสค์ โปรแกรม Bootstrap ที่ถูกอ่านขึ้นมาก็จะถูกเรียกทำงานเลย การทำงานคือการอ่านเอาระบบปฏิบัติการดอสมาลงบนหน่วยความจำแรมและโอนการทำงานให้กับดอสต่อไป

4. ในระบบปฏิบัติการซึ่งจะประกอบด้วยไฟล์โปรแกรม 2 ไฟล์ คือ IO.SYS และ MSDOS.SYS (หรือ IBMBIO.SYS และ IBMDOS.SYS) ก็จะถูกเรียกทำงาน

จากนั้นระบบปฏิบัติการดอสจะอ่านไฟล์ CONFIG.SYS ขึ้นมาพิจารณาถึงการติดตั้งพารามิเตอร์ของระบบ (เช่น ขนาดของบัฟเฟอร์ จำนวนไฟล์ที่เปิดได้สูงสุด เป็นต้น) และการติดตั้งดีไวซ์-ไดรเวอร์ต่าง ๆ เช่น ANSY.SYS ที่จะต้องโหลดลงหน่วยความจำของระบบ

5. หลังจากนั้นดอสจะโหลด COMMAND.COM มาทำงานต่อ ซึ่ง COMMAND.COM ก็คือโปรแกรมที่ควบคุมการติดต่อระหว่างผู้ใช้งานกับเครื่องโดยจะรอรับคำสั่งจากผู้ใช้และทำงานตามคำสั่งนั้น ๆ

6. ถ้ามีไฟล์ AUTOEXEC.BAT อยู่ ดอสจะอ่านและทำตามคำสั่งต่าง ๆ ที่บรรจุอยู่ในไฟล์นี้ แต่ถ้าไม่มีไฟล์นี้อยู่ดอสจะถามวันและเวลาจากผู้ใช้แทน

7. เมื่อหมดขบวนการข้างต้นแล้ว ระบบดอสจะแสดงเครื่องหมายเตรียมพร้อมและรอรับคำสั่งจากผู้ใช้งาน คำสั่งหลายคำสั่งเป็นคำสั่งภายในของดอส และคำสั่งภายนอกหรือเป็นชื่อของโปรแกรมไฟล์ .EXE .COM หรือ .BAT ซึ่งระบบดอสจะพยายามค้นหาไฟล์เหล่านี้ตามไดเรคทอรีย่อยต่าง ๆ ที่ติดตั้งเอาไว้ในพาธ (PATH) ถ้าพบไฟล์เหล่านั้นดอสจะอ่านเอาโปรแกรมนั้นลงสู่หน่วยความจำและโอนการทำงานให้ โปรแกรมเหล่านั้นบางครั้งอาจต้องการไฟล์โอเวอร์เลย์ (OVL) ร่วมในการทำงานด้วย ซึ่งไฟล์โอเวอร์เลย์มักจะมีนามสกุลเป็น .OVL .OV1 .OV2 ฯลฯ

8. ในโปรแกรมประยุกต์บางโปรแกรมที่ถูกโหลดมาทำงาน อาจจะเป็นโปรแกรมจำพวกแปลภาษา เช่น โปรแกรมแปลภาษาเบสิก เป็นต้น ซึ่งจะมีการอ่านไฟล์ชุดคำสั่งขึ้นมาแปลแล้วทำงาน หรือโปรแกรมประยุกต์สำเร็จรูปหลาย ๆ โปรแกรม เช่น ดีเบส โลตัส ก็มีความสามารถในการอ่านไฟล์ชุดคำสั่ง (ในกรณีโลตัส คือ มาโคร) ขึ้นมาแปลและทำงานตามชุดคำสั่งเหล่านั้น

จากลำดับขั้นตอนการทำงานของเครื่องดังกล่าวข้างต้น เราจะพบว่าถ้าหากไวรัสต้องการเข้าครอบครองระบบไวรัสคอมพิวเตอร์ควรจะเข้าเกาะติดตามจุดต่าง ๆ ในขั้นการทำงานของเครื่องโดยทำการดัดแปลงขั้นตอนบางขั้นตอนเสียใหม่ให้มีการเรียกหรือปลุกโปรแกรมไวรัสขึ้นมาก่อนแทรกเข้าไปในบางขั้นตอน ซึ่งต่อไปเราจะลองช่วยกันพิจารณาดูว่ามีจุดใดบ้างในแต่ละขั้นตอนที่ไวรัสคอมพิวเตอร์จะเข้าเกาะหรือแพร่พันธุ์ตัวเองเข้าไปในระบบได้

## โปรแกรมในรอมไบออส (BIOS ROM)

– ในส่วนนี้ไวรัสเข้าแพร่พันธุ์ไม่ได้แน่นอน เนื่องจากหน่วยความจำชนิดรอมจะถูกเขียนได้เพียงครั้งแรกครั้งเดียวเท่านั้น ดังนั้นโปรแกรมไวรัสจึงไม่สามารถจะทำการดัดแปลงโปรแกรมไบออสได้เลย สำหรับในหน่วยความจำ CMOS ซึ่งได้อธิบายไปแล้วว่าเป็นที่สำหรับเก็บข้อมูลไม่ใช่ที่อยู่ของโปรแกรม จึงไม่ใช่จุดที่ไวรัสจะเข้าเกาะติดเพื่อแพร่พันธุ์

## ในฮาร์ดดิสค์

– คือส่วนของตารางแบ่งส่วนและบูตเซกเตอร์ของพาร์ติชันที่มีระบบปฏิบัติการดอสอยู่ เป็นจุดหนึ่งที่ไวรัสคอมพิวเตอร์ชอบใช้เป็นที่อยู่ในการ

แพร่พันธุ์ เช่น ไวรัส Stoned Italian และ Mistake อยู่ในตารางแบ่งส่วน และไวรัส New Zealand เกาะอยู่ในบูตเซกเตอร์

## ในฟลอปปี้ดิสค์

– คือ บูตเซกเตอร์ ไวรัสหลายตัวชอบใช้เป็นที่แพร่พันธุ์

## ไฟล์ของระบบดอส

– คือ IO.SYS และ MSDOS.SYS เป็นจุดหนึ่งซึ่งอาจถูกใช้เป็นที่แพร่พันธุ์ของไวรัสได้ ถึงแม้ว่าในปัจจุบันยังไม่พบไวรัสตัวใดที่ใช้ไฟล์ทั้งสองเป็นที่เกาะแพร่พันธุ์ก็ควรระมัดระวังไว้ สำหรับในกรณีของไฟล์ CONFIG.SYS เป็นไฟล์ที่เก็บข้อความ (Text File) ซึ่งไวรัสไม่สามารถเข้าเกาะได้ แต่ไวรัสอาจจะทำการเพิ่มข้อความเพื่อให้ระบบโหลดเอาไวรัสที่ถูกเขียนมาในรูปของดีไวซ์-ไดรเวอร์ขึ้นมาทำงานก็ได้

## COMMAND.COM

– เป็นอีกจุดหนึ่งที่ไวรัสชอบใช้ ซึ่งอย่างน้อยก็พบไวรัส Lehigh ที่เกาะติดไฟล์นี้

## AUTOEXEC.BAT

– เป็นจุดที่ไวรัสอาจจะใช้เป็นที่แพร่พันธุ์ได้อีกจุดหนึ่ง แต่โดยปกติแล้วพบพวกโปรแกรมโทรจันมากกว่า

## โปรแกรมประยุกต์ .COM .EXE และ .OVL

– มีไวรัสมากมายหลายตัวที่ใช้ไฟล์เหล่านี้ แต่สำหรับไฟล์พวกโอเวอร์-เลย์ตอนนี้ยังไม่พบว่ารายงานไวรัสตัวใดใช้ไฟล์นี้ แต่ก็ควรระมัดระวังเพราะเป็นอีกจุดที่ไวรัสอาจใช้งานได้

## ไฟล์ชุดคำสั่งของโปรแกรมประยุกต์

– ยังไม่พบรายงานไวรัส แต่จากการที่มีผู้ทดลองแล้วพบว่าเป็นอีกจุดหนึ่งที่ไวรัสอาจใช้เป็นที่แพร่พันธุ์ได้เหมือนกัน

จากจุดต่างที่เราพิจารณากันแล้ว เพื่อเป็นการป้องกันการติดตั้งหรือแพร่-พันธุ์ไวรัสในระหว่างการทำงานใช้เครื่องเราจึงจะต้องคอยระมัดระวังสิ่งแปลกปลอมที่จะเข้าจู่โจมหรือเปลี่ยนแปลงข้อมูลในจุดเหล่านั้น ซึ่งเป็นเรื่องค่อนข้างยากที่จะต้องมาคอยเฝ้าเนื่องจากมีหลายจุดและหลายขั้นตอนที่ต้องระวัง และจากการที่ได้กล่าวไปแล้วข้างต้นในปัจจุบันชุดโปรแกรมต่อต้านไวรัสหลาย ๆ โปรแกรมก็มักจะมีโปรแกรมที่คอยระมัดระวังจุดเหล่านี้ให้เราอยู่ ซึ่งก็เป็นหน้าที่ของเราผู้ใช้ว่าควรจะเลือกโปรแกรมชุดใดที่จะป้องกันจุดเหล่านั้นครบมากกว่ากัน

## เป้าหมายการทำลายล้าง

หลังจากไวรัสเข้าครอบครองระบบได้แล้ว พฤติกรรมอีกอย่างหนึ่งที่ร้ายแรงและไวรัสส่วนใหญ่มักจะมีก็คือการทำลายในระบบเครื่องไมโครคอมพิวเตอร์ของเรามีจุดอ่อนอยู่มากมายที่ไวรัสอาจเข้าทำลายได้ ซึ่งเราจะพิจารณากันเป็นจุด ๆ ไปดังนี้

### 1. โปรแกรมไบออส

– ในส่วนนี้ไวรัสไม่สามารถทำลายได้ สำหรับหน่วยความจำซีมอส (CMOS) ซึ่งเก็บข้อมูลสำคัญของเครื่องไว้อาจจะถูกไวรัสทำลายข้อมูลดังกล่าวได้ โดยจะมีผลทำให้ระบบของเครื่องผิดไปและไม่สามารถทำงานต่อได้ การแก้ไขก็ทำโดยติดตั้งข้อมูลเดิมลงไปในหน่วย-ความจำซีมอส ซึ่งโดยส่วนใหญ่แล้วผู้ใช้งานมักจะจำข้อมูลดังกล่าวไม่ได้

### 2. ตารางแบ่งส่วนของฮาร์ดดิสค์ (Partition Table)

– เป็นข้อมูลส่วนสำคัญในการที่จะใช้งานฮาร์ดดิสค์และก็เป็นจุดสำคัญจุดที่ไวรัสจะเข้าทำลายได้ ซึ่งถ้าข้อมูลส่วนนี้ถูกทำลายฮาร์ดดิสค์ดังกล่าวจะไม่สามารถเรียกใช้งานได้อีกซึ่งก็หมายความว่าข้อมูลต่าง ๆ ในฮาร์ดดิสค์ไม่สามารถนำมาใช้งานได้อีกเลย

### 3. บูตเซกเตอร์ในฟลอปปี้ดิสค์

– ไวรัสอาจเข้าทำลายข้อมูลส่วนนี้ซึ่งจะมีผลทำให้แผ่นฟลอปปี้ดิสค์ดังกล่าวไม่สามารถใช้บูตระบบดอสได้อีก การแก้ไขก็ทำเพียงใช้คำสั่ง SYS.COM ของดอสเพื่อโอนระบบดอสกลับลงแผ่นอีกครั้ง

### 4. พื้นที่ส่วนสำคัญที่ใช้สำหรับจัดเก็บข้อมูลของดิสค์

– ได้แก่ พื้นที่ไดเรคทอรี และตาราง FAT เป็นต้น เป็นพื้นที่ของข้อมูลที่มีความสำคัญต่อการเก็บและค้นหาข้อมูล ซึ่งถ้าข้อมูลในพื้นที่เหล่านี้สูญหายหรือถูกทำลาย การเรียกค้นข้อมูลก็จะทำไม่ได้ ถึงแม้ว่าตัวข้อมูลยังคงอยู่ในดิสค์ก็ตาม

ในระบบไมโครคอมพิวเตอร์จริงแล้วมีจุดสำคัญมากมายที่ไวรัสจะเข้าโจมตีและทำลายได้ ที่กล่าวมาก็เป็นเพียงบางส่วนที่สำคัญเท่านั้น ในชุดโปรแกรมต่อต้านไวรัสคอมพิวเตอร์ก็มักจะมีโปร-แกรมสำหรับติดตามและระมัดระวัง

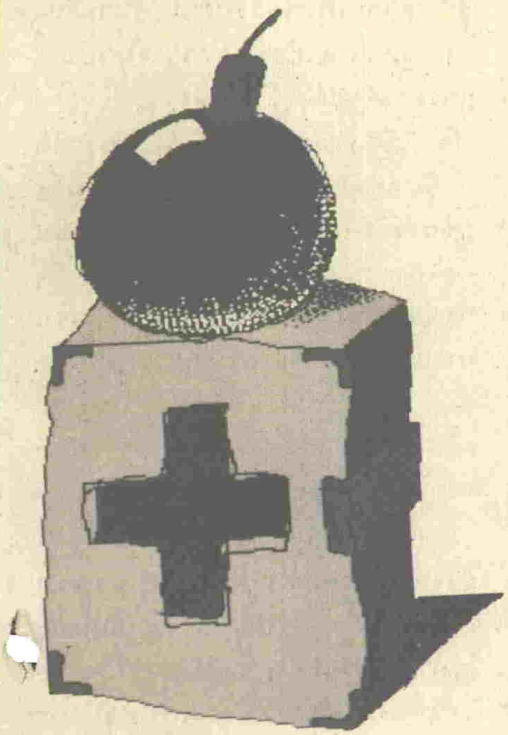
เหตุการณ์ที่จะเป็นการทำลายต่อจุดสำคัญนี้มาให้ด้วย

## ประเภทของซอฟต์แวร์

ในตลาดไมโครคอมพิวเตอร์ปัจจุบันมีซอฟต์แวร์ต่อต้านไวรัสจำหน่ายอยู่มากมายหลายโปรแกรม แต่ละชุดก็มีคุณสมบัติโดดเด่นต่างกันออกไปบ้างอย่างไรก็ตาม ในชุดโปรแกรมหลายโปรแกรมก็มีคุณสมบัติพื้นฐานเหมือนกัน ซึ่งพอจะจำแนกโปรแกรมต่อต้านไวรัสออกได้หลาย ๆ ประเภท ตามวิธีการทำงานได้ดังนี้

### โปรแกรมตรวจสอบไวรัสที่ไม่รู้จักมาก่อน

โปรแกรมพวกนี้จะใช้วิธีการคำนวณหาค่าผลรวมของ (checksum) ของเนื้อไฟล์ที่เป็นโปรแกรมที่สามารถเรียกใช้ทำงานได้ในระบบ โดยทำการเก็บข้อมูลผลรวมของไฟล์เหล่านี้เอาไว้เป็นตารางสำหรับเปรียบเทียบในการคำนวณครั้งใหม่ ซึ่งถ้าค่าผลรวมที่คำนวณใหม่ไม่ตรงกับข้อมูลผลรวมเดิมที่เก็บไว้นั้นหมายถึงไฟล์โปรแกรมนั้นถูกไวรัสเกาะติดแล้ว



โดยปกติแล้วโปรแกรมพวกนี้มักจะเป็นโปรแกรมธรรมดาที่ไม่ตอบสนองทันทีทันใด หมายความว่าถ้าไวรัสเกาะติดไฟล์แล้วเมื่อเรียกโปรแกรมชุดนี้ทำงานจึงค่อยทราบว่ามีไวรัสเกาะติดไฟล์

การติดตั้งโปรแกรมที่ทำงานในลักษณะนี้ต้องมีความระมัดระวัง คือ ก่อนจะติดตั้งโปรแกรมนี้ลงระบบ ระบบควรจะสะอาดเสียก่อน (ไม่มีไวรัสติดอยู่) เพื่อความแน่ใจควรทำตามขั้นตอนดังนี้

1. เริ่มติดตั้งระบบใหม่ โดยเริ่มตั้งแต่ทำการฟอร์แมตฮาร์ดดิสก์ใหม่ โดยเริ่มจากการฟอร์แมตระดับต่ำ (Low level format) แต่อย่าลืมสำรองข้อมูล (เฉพาะข้อมูล) ขึ้นมาก่อน
2. ติดตั้งโปรแกรมหรือซอฟต์แวร์ต่าง ๆ ตามต้องการ (จากแผ่นดิสก์ต้นฉบับเท่านั้น)
3. ใช้โปรแกรมสแกนหาไวรัสที่รู้จักก่อน เพื่อความแน่ใจว่าไม่มีไวรัสอยู่
4. จากนั้นจึงเรียกโปรแกรมให้ทำการคำนวณหาผลรวมเพื่อเก็บเอาไว้เปรียบเทียบต่อไป

ข้อดีของโปรแกรมต่อต้านไวรัสประเภทนี้ คือสามารถใช้ตรวจสอบการติดไวรัสทุกตัวไม่ว่าไวรัสตัวเก่าหรือไวรัสตัวใหม่ได้อย่างแน่นอน และนอกจากนั้นโปรแกรมประเภทนี้บางโปรแกรมในปัจจุบัน ยังใช้วิธีการนี้กับข้อมูลในส่วนของบูตเซกเตอร์ และตารางแบ่งส่วน (Partitable) ของฮาร์ดดิสก์ด้วย ซึ่งทำให้สามารถตรวจสอบไวรัสประเภทที่ติดบูตเซกเตอร์และตารางแบ่งส่วนได้

วิธีการหาผลรวมมีหลายวิธีการ (Algorithm) เช่น การหาผลรวมแบบง่ายด้วยการบวกข้อมูลธรรมดา (Simple checksum) หรือการคำนวณหาค่า CRC (Cyclie Redundance check) แต่อย่างไรก็ตาม การคำนวณหาผลรวมตามวิธีทั้งสองที่กล่าวไม่นิยมนำมาใช้ในโปรแกรมประเภทนี้ เพราะวิธีการคำนวณเป็นที่เปิดเผยและทราบกันทั่วไป ซึ่งผู้เขียนโปรแกรมไวรัสเองก็ทราบและถ้าจะเขียนโปรแกรมไวรัสให้แก้ไขหรือเพิ่มข้อมูลบางส่วนลงไปในไฟล์ที่เกาะเพื่อให้ได้ค่าคำนวณตามวิธีการที่ใช้มีค่าเท่าเดิมก่อนหน้าที่จะเกาะติด ซึ่งจะมีผลทำให้โปรแกรมนี้ไม่สามารถตรวจสอบได้ ดังนั้นวิธีการคำนวณหาค่าผลรวมของโปรแกรมต่อต้านประเภทนี้ส่วนใหญ่จึงเป็นวิธีการคำนวณลับเฉพาะเพื่อป้องกันปัญหาดังกล่าว

### โปรแกรมตรวจหาไวรัสที่รู้จัก

การทำงานของโปรแกรมต่อต้านไวรัสประเภทนี้จะใช้วิธีการสแกนหาลักษณะเฉพาะ (Signature) ของไวรัสแต่ละตัวที่ทราบในเนื้อไฟล์หรือบริเวณที่บูตเซกเตอร์ ตารางแบ่งส่วน ซึ่งลักษณะเฉพาะของไวรัสได้มาจากการวิเคราะห์คุณสมบัติของไวรัสตัวนั้น ๆ อย่างละเอียด แล้วเก็บเป็นข้อมูลเอาไว้สำหรับเปรียบเทียบ

อย่างไรก็ตาม โปรแกรมประเภทนี้จะค้นหาได้เฉพาะไวรัสที่โปรแกรมรู้จักเท่านั้น แต่สำหรับไวรัสตัวใหม่ที่เกิดขึ้นมาก็จะตรวจหาไม่ได้ ซึ่งปัญหานี้เป็นข้อเสียจุดหนึ่งสำหรับโปรแกรมประเภทนี้ ซึ่งผู้ใช้งานต้องคอยตามโปรแกรมรุ่นใหม่ที่มีการแก้ไขและเพิ่มข้อมูลของไวรัสตัวใหม่เข้าไป แต่ในบางโปรแกรมก็แก้ปัญหานี้โดยยอมให้ผู้ใช้งานสามารถเพิ่มลักษณะเฉพาะของไวรัสตัวใหม่ที่ผู้ใช้งานพบเข้าไปในโปรแกรมได้เอง โดยผู้ใช้ต้องเป็นผู้วิเคราะห์และ

หาลักษณะเฉพาะของไวรัสตัวใหม่เอง หรืออาจจะหาได้จากวารสาร "Virus Bulletin" ซึ่งพิมพ์ออกทุกเดือน โดยภายในวารสารจะมีรายละเอียดของไวรัสตัวใหม่ ๆ ที่เกิดขึ้น และลักษณะเฉพาะที่เป็นกลุ่มตัวเลขฐานสิบหก

ความยาวของลักษณะเฉพาะหรือกลุ่มตัวเลขฐานสิบหกเป็นสิ่งที่สำคัญเหมือนกัน ถ้าใช้จำนวนตัวเลขสั้นหรือน้อยไปโอกาสที่โปรแกรมสแกนหาข้อมูลในไฟล์ก็อาจจะมีโอกาสตรงกับกลุ่มตัวเลขที่ใช้ก็ได้ ซึ่งก็จะทำให้เกิดความเข้าใจผิดคิดว่าพบไวรัส ดังนั้นจำนวนตัวเลขในกลุ่มลักษณะเฉพาะควรจะมีความยาวพอสมควร ตามปกติจะอยู่ระหว่าง 10 ถึง 16 ตัว

โปรแกรมประเภทนี้ส่วนใหญ่แล้วจะทำงานช้า ถึงแม้บางโปรแกรมจะใช้วิธีการเพิ่มความเร็ว โดยค้นหาข้อมูลเฉพาะในบริเวณที่ไวรัสเกาะติดเท่านั้น ไม่ใช้ทั้งไฟล์หรือทั้งบริเวณบูตเซกเตอร์ตารางแบ่งส่วนก็ตาม แต่ว่าไวรัสแต่ละตัวก็จะมีบริเวณที่ใช้เกาะติดไม่เหมือนกัน ซึ่งทำให้การค้นหาซับซ้อนกว่าวิธีธรรมดา

คุณสมบัติอีกอันหนึ่งซึ่งมักจะติดมาด้วยกับโปรแกรมประเภทนี้ก็คือความสามารถในการดึงเอาไวรัสที่เกาะติดอยู่ (ไม่ว่าจะเป็นในไฟล์บูตเซกเตอร์ หรือตารางแบ่งส่วน) ออกจากบริเวณนั้น ๆ โดยที่ไฟล์หรือดิสก์ (ฮาร์ดดิสก์) นั้นยังคงใช้งานได้เหมือนเดิม แต่ในบางครั้งหลังจากที่ไฟล์หรือดิสก์นั้นได้รับการรักษาโดยนำเอาไวรัสออกไปแล้วก็ตาม ก็อาจจะใช้งานไม่ได้เหมือนเดิม ดังนั้นวิธีการง่ายและแน่นอนกว่าในการกำจัดไวรัสออกไปนั้นทำโดยการลบไฟล์หรือฟอร์แมตดิสก์นั้นเสียใหม่ และนำเอาซอฟต์แวร์จากแผ่นต้นฉบับมาใส่แทน

โปรแกรมต่อต้านไวรัสประเภทนี้มีประโยชน์มากสำหรับใช้ในการตรวจสอบดิสก์ที่บรรจุซอฟต์แวร์มาใหม่ว่ามีไวรัสตัวใดที่รู้จักติดมาบ้างก่อนจะนำซอฟต์แวร์นั้นไปใช้งาน

## โปรแกรมติดตามและป้องกันไวรัส

ลักษณะการทำงานของโปรแกรมนี้จะเป็นโปรแกรมที่ทำงานตลอดเวลา โดยคอยตรวจสอบการทำงานระบบ (ทั้งดอสและไบออส) ทั้งหมด รวมทั้งการทำงานที่เกี่ยวข้องกับดิสก์ ซึ่งโปรแกรมประเภทนี้จะเป็นพวกโปรแกรมเรสซิเดนต์

การติดตามการทำงานของโปรแกรมนี้มีทั้งติดตามระมัดระวังอันตรายในจุดบริเวณสำคัญของระบบที่ไวรัสจะเข้าโจมตีได้ รวมทั้งการป้องกันการแพร่พันธุ์ของไวรัสเข้าสู่ระบบด้วย โปรแกรมประเภทนี้บางโปรแกรมจะมีการระมัดระวังและการป้องกันอย่างเข้มแข็ง แต่อย่างไรก็ตาม บริเวณสำคัญของระบบเหล่านั้นไม่ใช่มีแต่เพียงไวรัสเท่านั้นที่จะเข้ากระทำ ในบางครั้งระบบเองหรือโปรแกรมประยุกต์บางโปรแกรมก็ต้องการเข้ากระทำต่อข้อมูลบริเวณนั้น เมื่อบริเวณเหล่านั้นถูกกระทำให้เปลี่ยนแปลง โปรแกรมก็จะร้องเตือนและแสดงข้อความแจ้งต่อผู้ใช้งานว่ากำลังจะเกิดอะไรต่อบริเวณนั้น ให้ผู้ใช้ตัดสินใจว่าจะทำงานต่อหรือยกเลิกการทำงาน ซึ่งบ่อยครั้งโปรแกรมประเภทนี้จะสร้างความรำคาญให้กับผู้ใช้มาก ดังนั้นโปรแกรมพวกนี้หลาย ๆ โปรแกรมก็ยอมให้ผู้ใช้ปรับแต่งบางจุดได้ การติดตามป้องกันยิ่งมากจุดยิ่งทำให้ประสิทธิภาพของระบบลดลง และบางครั้งก็มีปัญหาไม่สามารถใช้กับเน็ตเวอร์กหรือกับโปรแกรมประยุกต์ตัวอื่นได้

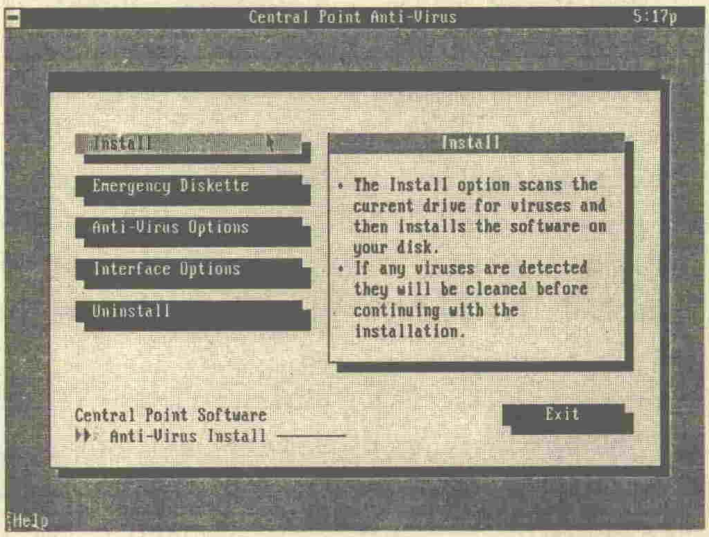
โปรแกรมไวรัสที่ฉลาด ๆ บางตัวก็สามารถที่จะหลุดรอดจากการติดตามของโปรแกรมประเภทนี้ได้ ซึ่งส่วนใหญ่แล้วโปรแกรมต่อต้านไวรัสพวกนี้จะคอยติดตามการทำงานของการเขียนและอ่านข้อมูลจากดิสก์ ดังนั้นหากโปรแกรมไวรัสสามารถเปลี่ยนอินเตอร์รัพต์เวกเตอร์ของดอสหรือของไบออสในตารางอินเตอร์รัพต์มาชี้ที่ตัวไวรัสเองทั้งหมด ก็จะสามารถหลุดรอดจากการติดตามของโปรแกรมประเภทนี้ได้

## โปรแกรมฉีดวัคซีน

โปรแกรมต่อต้านไวรัสประเภทนี้เท่าที่พบในปัจจุบันมีการทำงานอยู่ 2 แบบ โดยแบบแรกนั้นโปรแกรมวัคซีนจะทำการดัดแปลงไฟล์ที่เป็นโปรแกรม บูตเซกเตอร์ หรือตารางแบ่งส่วนให้มีคุณสมบัติในการตรวจสอบตัวเองได้ ซึ่งโปรแกรมวัคซีนจะคำนวณหาค่าผลรวม (check sum) แล้วนำโปรแกรมเล็ก ๆ สำหรับตรวจสอบผลรวมกับค่าผลรวมที่คำนวณได้เก็บเอาไว้ในบริเวณดังกล่าว โดยลักษณะการเก็บจะต้องให้โปรแกรมส่วนนี้ถูกเรียกก่อนโปรแกรมเดิม ซึ่งจะต้องทำการเปลี่ยนแปลงโครงสร้างไฟล์โปรแกรมบูตเซกเตอร์ และตารางแบ่งส่วน เรียกวิธีการทำงานเช่นนี้ว่า การฉีดวัคซีนต่อต้านไวรัส โปรแกรมวัคซีนจะมีข้อจำกัดเพราะเนื่องจากการฉีดวัคซีนต้องทำการเปลี่ยนแปลงโครงไฟล์ ซึ่งการทำเช่นนี้จะใช้ไม่ได้กับโปรแกรมบางประเภท ที่โครงสร้างโปรแกรมที่ซับซ้อน เช่น โปรแกรมที่ต้องมีโอเวอร์เลย์ หรือโปรแกรมประเภทที่มีการตรวจสอบขนาดและค่าผลรวมอยู่ในตัวเองแล้ว

ส่วนโปรแกรมวัคซีนแบบที่สองต่างกับโปรแกรมวัคซีนประเภทแรกก็คือตัววัคซีนที่ใช้ฉีดเป็นข้อมูลลักษณะเฉพาะของไวรัส (Signature) เพราะไวรัสหลาย ๆ ตัวก่อนจะแพร่พันธุ์มักจะ

ตรวจสอบก่อนเสมอว่าบริเวณที่จะใช้เกาะติดได้เคยเกาะติดมาแล้วหรือยัง เพื่อป้องกันการติดซ้ำ (ถ้ายังจำได้ไวรัส SUMsDos ที่ติดไฟล์ซ้ำแล้วซ้ำอีกจนขนาดไฟล์ใหญ่โตเป็นที่ผิดสังเกต) โปรแกรมวัคซีนแบบนี้ไม่แนะนำให้ใช้งาน เนื่องจากการทำลักษณะนี้ไม่ใช่วิธีการป้องกันที่ถาวร นอกจากนั้นไฟล์ที่ถูกฉีดวัคซีนแล้วอาจจะทำให้เกิดความเข้าใจผิดให้กับโปรแกรมตรวจสอบไวรัสโดยการสแกนก็ได้




รูปที่ 2 เมนูขณะติดตั้ง CPAV

## CPAV โปรแกรมต่อต้านไวรัส

หลังจากแนะนำให้ท่านผู้อ่านทราบถึงคุณสมบัติต่าง ๆ ของโปรแกรมต่อต้านไวรัสมากมายจนถึงขั้นนี้ ก็เพื่อที่จะให้เป็นข้อมูลสำหรับผู้อ่านใช้ในการตัดสินใจพิจารณาเลือกซื้อโปรแกรมต่อต้านไวรัสที่จะนำไปใช้งาน และจากนี้ก็จะเป็นการแนะนำโปรแกรมต่อต้านไวรัส CPAV (Central Point Anti-Virus) โปรแกรมหนึ่งที่น่าสนใจ โดยจะได้เล่าถึงรายละเอียดของคุณสมบัติการต่อต้านไวรัสที่ CPAV มีให้ท่านผู้อ่านได้ทราบ

## CPAV ชุดรวมเบ็ดเสร็จ

ถ้าจำไม่ผิด ผู้เขียนเห็นซอฟต์แวร์เทอร์โบแอนตี้ไวรัส (TNT-VIRUS) ตอนนั้นยังเป็นโปรแกรมขั้นทดลองอยู่ ซึ่งการทำงานหลาย ๆ ส่วนเหมือนกับ CPAV อาจจะเป็น CPAV ถอดแบบการทำงานมาก็ได้ จากที่ได้ทดลองใช้ CPAV ดูแล้วพบว่าทำงานได้เป็นที่น่าพอใจ (ซึ่งผู้เขียนก็คิดว่าน่าเป็นเช่นนั้น เพราะผู้พัฒนาซอฟต์แวร์ตัวนี้คือ บริษัท Central Point Software ผู้พัฒนาซอฟต์แวร์ PCTOOLS) ในชุดซอฟต์แวร์ของ CPAV มีโปรแกรมประกอบอยู่หลายตัวที่สนับสนุนการทำงานในการต่อต้านไวรัสได้หลาย ๆ ระดับ ซึ่งสามารถป้องกันไวรัสได้ทั้งไวรัสที่รู้จักและไม่รู้จัก ซึ่งได้แก่ โปรแกรม Bootsafe .VSafe และ VWate ส่วนโปรแกรมหลักคือ CPAV นั้นเป็นโปรแกรมสำหรับใช้สแกนและตรวจสอบไฟล์ รวมทั้งสามารถกำจัดไวรัสออกจากไฟล์พบได้ด้วย รายละเอียดของโปรแกรมแต่ละตัวมีดังนี้

## Bootsafe

ตามที่ทราบแล้วว่ามีไวรัสหลายตัวที่อาศัยพื้นที่บริเวณบูตเซกเตอร์และตารางแบ่งส่วนเป็นที่อยู่ โปรแกรม Bootsafe จะช่วยปกป้องพื้นที่ส่วนนี้ให้ ซึ่งในคู่มือของโปรแกรมแนะนำว่าควรจะติดตั้งโปรแกรม Bootsafe เอาไว้ในทุกดิสค์ที่ใช้บูตระบบ (โดยก๊อบปี้ไฟล์ Bootsafe.exe เอาไว้ในดิสค์และเรียกโปรแกรม Bootsafe ไว้ใน Autoexec.bat ด้วย) โดยเฉพาะอย่างยิ่งในฮาร์ดดิสค์

เมื่อ Bootsafe ถูกเรียกจาก Autoexec.bat ไฟล์จะเริ่มอ่านเอาข้อมูลในบูตเซกเตอร์และตารางแบ่งส่วนจากดิสค์ในขณะนั้น ซึ่งข้อมูลในบูตเซกเตอร์และตารางแบ่งส่วนได้ถูกเก็บไว้แล้วเมื่อตอนติดตั้งโปรแกรมครั้งแรก ถ้ามีอะไรเปลี่ยนแปลงจากข้อมูลเดิมโปรแกรมจะรายงานและหยุดการทำงาน ซึ่งเท่ากับเป็นการหยุดการทำงานของไวรัสถ้ามันอาศัยอยู่ในบูตเซกเตอร์และตารางแบ่งส่วน

นอกจากนั้นโปรแกรม Bootsafe ยังสามารถก๊อบปี้เก็บเอาข้อมูลจากบูตเซกเตอร์และตารางแบ่งส่วนไว้ในแผ่นฟลอปปี้ดิสค์ (รวมทั้งข้อมูลในหน่วยความจำแรม CMOS ด้วย) ซึ่งเป็นการป้องกันฮาร์ดดิสค์เสียหาย โดยแผ่นฟลอปปี้ดิสค์ดังกล่าวจะต้องเก็บรักษาเอาไว้ หากเกิดปัญหาขึ้นกับฮาร์ดดิสค์ในพื้นที่ส่วนนี้ก็สามารถใช้โปรแกรม Bootsafe ซ่อมแซมได้โดยอาศัยข้อมูลที่เก็บไว้ก่อนแล้ว

การเก็บข้อมูลจากบูตเซกเตอร์และตารางแบ่งส่วนสามารถทำได้ 2 วิธี ซึ่งวิธีแรกทำได้ในขณะติดตั้งซอฟต์แวร์ CPAV (ดูรูปที่ 2 ประกอบ) โดยในเมนูของการติดตั้งโปรแกรมจากข้อมูลเลือกให้สร้างแผ่นดิสค์ฉุกเฉิน ส่วนวิธีที่ 2 นั้น

ทำโดยเรียกโปรแกรม Bootsafe โดยตรง การใช้งาน Bootsafe ทำได้ดังนี้

– เรียกโปรแกรมเพื่อตรวจสอบความผิดปกติที่จะเกิดขึ้นกับดิสก์ในส่วนของบูตเซกเตอร์และตารางแบ่งส่วน ทำได้โดยเรียงชื่อ Bootsafe เช่น

C:\ >Bootsafe <Enter>

จะตรวจสอบดิสก์ที่ใช้งานอยู่ (ในกรณีคือไดรฟ์ C) ในกรณีต้องการตรวจสอบไดรฟ์อื่นก็สามารถทำได้โดยใส่ชื่อไดรฟ์ตามหลัง เช่นต้องการตรวจสอบไดรฟ์ D:

C:\ >Bootsafe D:

หรือถ้าต้องการตรวจสอบหลาย ๆ ไดรฟ์ก็สามารถสั่งงานได้ทีเดียว

C:\ >Bootsafe C: D: E:

– การเก็บข้อมูลจากบูตเซกเตอร์และตารางแบ่งส่วน ลงในแผ่นฟลอปปี้ดิสก์เพื่อเอาไว้ซ่อมแซมเมื่อฮาร์ดดิสก์ถูกไวรัสโจมตี ข้อมูลที่เก็บนอกจากบูตเซกเตอร์และตารางแบ่งส่วนแล้วยังเก็บข้อมูลในหน่วยความจำ CMOS ให้ด้วย ข้อมูลทั้งหมดจะถูกเขียนลงในแผ่นฟลอปปี้ดิสก์ไดรฟ์ A การเรียกใช้โปรแกรม Bootsafe ในกรณีนี้จะต้องตามหลังด้วยชื่อไดรฟ์ที่ต้องการเก็บด้วย /M ตัวอย่างเช่น

C:\ >Bootsafe C: /M

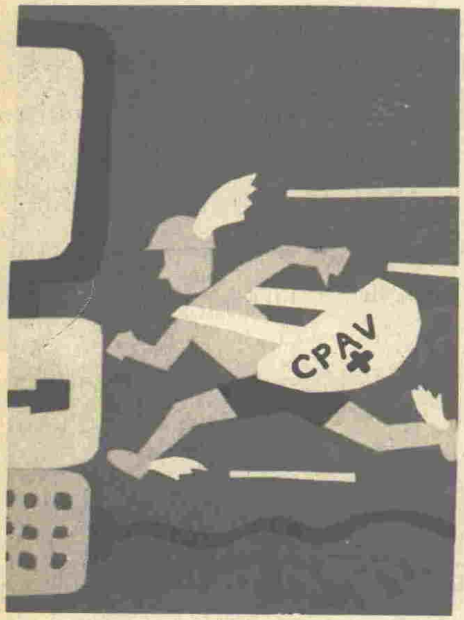
โปรแกรมจะถามให้ใส่แผ่นฟลอปปี้ดิสก์ที่ไดรฟ์ A (แผ่นดิสก์ควรจะเป็นแผ่นที่ฟอร์แมตใหม่) ชื่อไฟล์สำหรับเก็บข้อมูลจะมีชื่อไดรฟ์นำหน้า ดังในกรณีข้างต้นจะได้ไฟล์ CBOOT.CPS (และ CMOS.cps) ดังนั้นแผ่นฟลอปปี้ดิสก์หนึ่งสามารถใช้เก็บบูตเซกเตอร์และตารางแบ่งส่วนของฮาร์ดดิสก์ตัวอื่นที่มีเพิ่มในระบบได้อีกด้วย เช่น ต้องการเก็บไดรฟ์ E

C:\ >Bootsafe E: /M

ไฟล์ที่เกิดในแผ่นจะเป็น EBOOT.CPS

– ซ่อมแซมหรือคืนข้อมูลในบูตเซกเตอร์และตารางแบ่งส่วน ในกรณีนี้ควรจะทำก็ต่อเมื่อฮาร์ดดิสก์เกิดความเสียหายเท่านั้น โดยเรียกโปรแกรม Bootsafe โปรแกรมจัดการหน่วยความจำ (Memory Management)

A:\ >Bootsafe C: /R




## VSafe และ VWatch

โปรแกรมทั้งสองเป็นโปรแกรมที่ทำงานในลักษณะโปรแกรมเรสซิเดนต์สำหรับคอยเฝ้าติดตามไวรัส ทั้ง VSafe และ VWatch จะใช้งานพร้อมกันไม่ได้ ต้องเลือกเอาอย่างใดอย่างหนึ่ง เพราะโปรแกรมทั้งสองมีการทำงานที่เหมือนกัน ต่างกันเพียงความสะดวกในการใช้งานและข้อจำกัดของการทำงาน ซึ่งการเลือกใช้ต้องพิจารณาถึงขนาดของหน่วยความจำในระบบ เพราะ VSafe จะมีขนาดโปรแกรมที่ใหญ่กว่า VWatch

VSafe เป็นโปรแกรมสำหรับป้องกันและต่อต้านการแพร่พันธุ์ของไวรัส VSafe เมื่อโหลดลงหน่วยความจำจะกินเนื้อที่ไปประมาณ 22 กิโลไบต์ การทำงาน VSafe จะเฝ้าดูระบบตลอดเวลาสำหรับเหตุการณ์ที่น่าสงสัยและจะเป็นอันตรายต่อระบบ เกิดการกระตุ้นจากไวรัสทั้งพันธุ์เก่าหรือพันธุ์ใหม่ โปรแกรม VSafe จะแสดงข้อความเตือนและจะถามผู้ใช้งานเครื่องให้เลือกว่าจะทำงานต่อหรือจะเริ่มระบบใหม่หรือจะยกเลิกการทำงานดังกล่าว โปรแกรม VSafe สามารถปรับแต่งการทำงานได้ถึง 8 อย่าง ซึ่งการเฝ้าคอยดูการทำงานของระบบและการร้องเตือนพร้อมข้อความบางครั้งอาจสร้างความรำคาญให้ผู้ใช้ได้ โปรแกรม VSafe จึงยอมให้ผู้ใช้สามารถปรับแต่งการทำงานได้ด้วย

ในกรณีที่เครื่องมีหน่วยความจำแบบขยาย (Extended) สามารถจะใช้โปรแกรมจัดการหน่วยความจำ (Memory Management) โหลดเอา VSafe โอนไว้ยังหน่วยความจำตอนบนได้

VWatch เป็นโปรแกรมป้องกันไวรัสสำหรับเครื่องที่หน่วยความจำแรมไม่มากพอ VWatch จะกินหน่วยความจำไปประมาณ 8 กิโลไบต์ เมื่อมีการเรียกใช้งานโปรแกรมใด ๆ หรือมีการใช้งานแผ่นดิสก์แผ่นใหม่เข้ามาในระบบ โปรแกรม VWatch จะตรวจสอบเฉพาะไวรัสที่รู้จัก ซึ่งถ้าหากพบโปรแกรมจะแสดงข้อความเตือนและจะหยุดการทำงานของระบบทันที

ทั้ง VSafe และ VWatch สามารถติดตั้งได้เป็น 2 ลักษณะคือ ติดตั้งแบบไดรเวอร์และเรียกโปรแกรม .COM ขึ้นทำงานตามธรรมดา ซึ่งต้องการติดตั้งแบบไดรเวอร์ให้ติดตั้งไว้ในไฟล์ CONFIG.SYS ดังนี้

DEVICE = VSAFE.SYS
หรือ DEVICE = VWATCH.SYS

แต่ถ้าจะติดตั้งแบบโปรแกรมธรรมดาให้ใส่ชื่อโปรแกรมเอาไว้ในไฟล์ AUTOEXEC.BAT แทน การติดตั้งแบบโปรแกรมธรรมดามีข้อดีคือสามารถจะยกเลิกหรือถอดเอาโปรแกรมออกจากหน่วยความจำได้

– การติดตั้ง VSafe หรือ VWatch ทำได้โดยเรียกชื่อโปรแกรมดังนี้

C:\ >VSafe
หรือ C:\ >VWatch

– การปรับแต่งการทำงานของ VSafe ทำได้ 2 วิธี วิธีแรกทำได้โดยเรียกโปรแกรมที่ติดตั้งไปแล้วขึ้นด้วยการกดแป้นพิมพ์ Alt กับ V (สามารถปรับเปลี่ยนตัว V เป็นแป้นอื่นได้ขณะติดตั้ง) ซึ่งจะปรากฏหน้าต่างที่จะแสดงข้อเลือกดังรูปที่ 3 การปรับแต่งทำได้ด้วยการเลือกหมายเลขตามเมนู สำหรับวิธีการปรับแต่งแบบที่สองใช้เฉพาะครั้งแรกสุดที่ทำการเรียก VSafe ทำงานด้วยตามสวิตช์ตัวเลขพร้อมตัวอักษร + (ให้มีการตรวจสอบ) และอักษร – (ไม่มีการตรวจสอบ) ดังตัวอย่าง

C:\ >VSafe /1+/–/3–/4+/5+/6+/7+/8–

VSafe สามารถปกป้องได้ 8 เหตุการณ์ดังนี้

1. HD Low level format :

– เตือนเมื่อมีเหตุการณ์ที่จะฟอร์แมตฮาร์ดดิสก์ในระดับล่าง

2. Resident :

– เตือนเมื่อมีโปรแกรมใดก็ตามจะฝังตัวลงหน่วยความจำ (เรสซิเดนต์) เนื่องจากไวรัสหลาย ๆ ตัวเป็นโปรแกรมพวกเรสซิเดนต์

3. General Write Protect :

– เตือนจะมีการเขียนข้อมูลลงดิสก์ การทำงานแบบนี้จะช่วยป้องกันไวรัสที่ชอบแพร่พันธุ์ด้วยการเกาะไฟล์ได้อย่างแน่นอน

4. Check executable files :

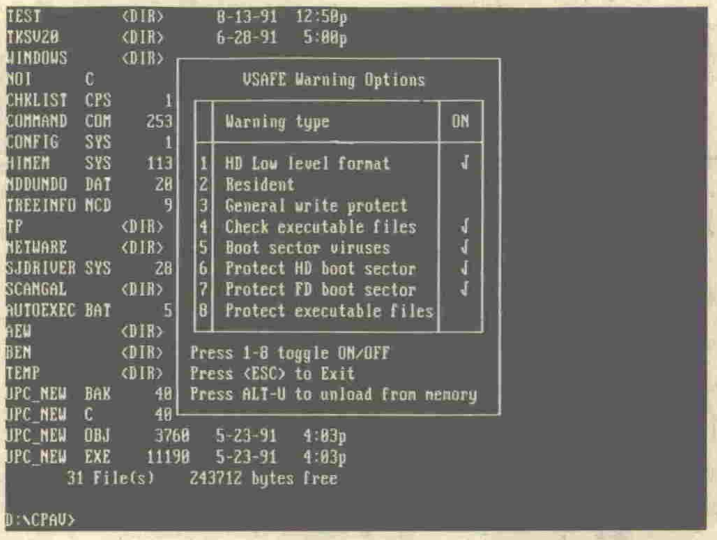
– ตรวจสอบไฟล์ทุกไฟล์ที่กำลังถูกเรียกขึ้นมาทำงานโดยดอส เพื่อค้นหาไวรัสเท่าที่รู้จัก

5. Boot Sector Virus :

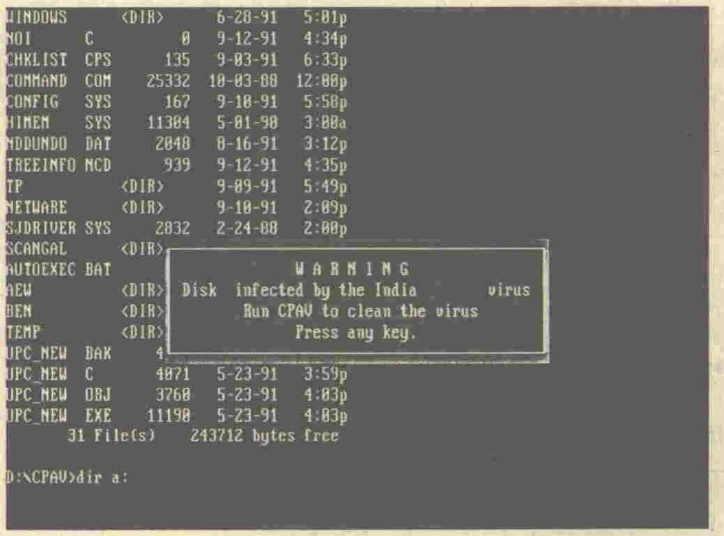
– ตรวจสอบแผ่นดิสก์ทุกแผ่นที่จะนำมาใช้ในระบบสำหรับไวรัสที่รู้จักดังในรูปที่ 4

6. Protect HD boot sector :

– เตือนเมื่อมีเหตุการณ์ที่พยายาม




รูปที่ 3 โปรแกรม VSafe สามารถปรับแต่งการทำงานได้ 2 วิธีที่ในรูปแสดงการปรับแต่งการทำงานโดยกดแป้น Alt-V ซึ่งจะแสดงหน้าต่างแสดงเมนูให้เลือกกดตัวเลขในหัวข้อที่ต้องการเพื่อเปลี่ยนการทำงานตามต้องการ




รูปที่ 4 การทำงานของ VSafe จะตรวจสอบแผ่นดิสก์ทุกแผ่นที่จะถูกใช้งาน กรณีในรูปแผ่นฟลอปปี้ที่ใส่เข้าใหม่มีไวรัส โปรแกรม VSafe จะร้องเตือนทันที

จะเขียนข้อมูลในบูตเซกเตอร์ของฮาร์ดดิสก์และตารางแบ่งส่วน

7. Protect FD bootsector :

– เตือนเมื่อมีเหตุการณ์ที่พยายามจะเขียนข้อมูลลงในบูตเซกเตอร์ของฟลอปปี้ดิสก์

8. Protect executable :

– เตือนเมื่อมีเหตุการณ์ที่พยายามเปลี่ยนแปลงโครงสร้างของไฟล์ที่เป็นโปรแกรม

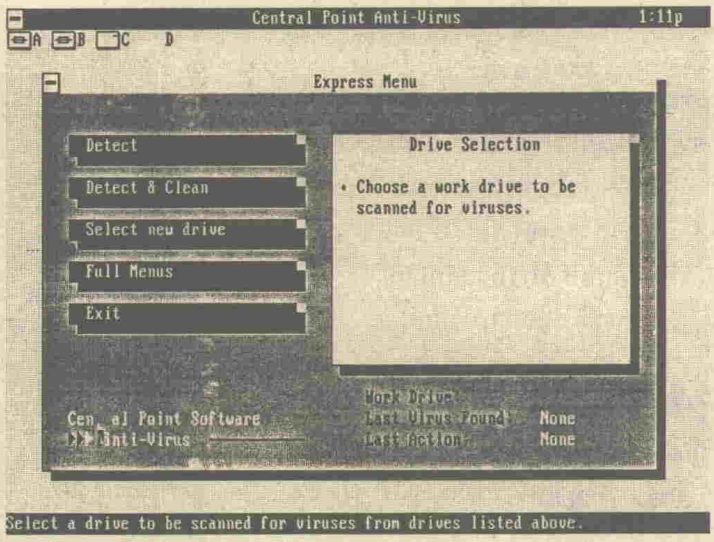
– การถอนโปรแกรม VSafe ออกจากหน่วยความจำ สามารถทำได้เช่นเดียวกันกับโปรแกรมเรสซิเดนต์ทั่วไป การถอนโปรแกรมออกจากหน่วยความจำจะต้องถอดโปรแกรมเรสซิเดนต์โปรแกรมอื่น (ที่ถูกติดตั้งหลัง VSafe) ออกให้หมดก่อน จากนั้นให้กด Alt กับ V เพื่อเรียกเมนูของ VSafe ขึ้นมา (หรือ Alt กับแป้นพิมพ์อื่นตามที่ติดตั้งเอาไว้ในตอนแรก) แล้วจึงกด Alt กับ U เพื่อถอด VSafe ออก หรืออาจจะทำการเรียกจากดอสธรรมดาได้ดังนี้

C:\ >Vsafte/u

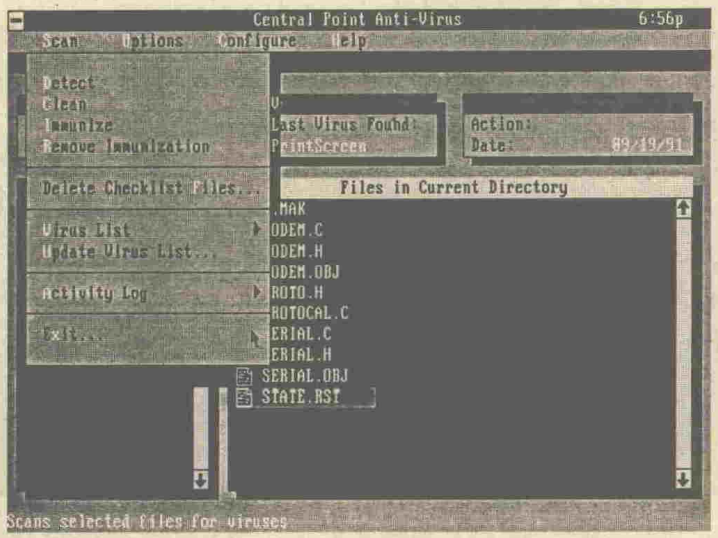
หรือ C:\ >VWatch/u

## สแกนหาไวรัสด้วย CPAV

โปรแกรม CPAV.EXE เป็นเมนหลักที่ใช้สำหรับสแกนหาไวรัสที่รู้จัก (ตามคู่มืออ้างว่ารู้จักไวรัสมากกว่า 600 ตัว) นอกจากนั้นยังสามารถแก้ไขไฟล์ที่ติดไวรัสให้กลับคืนสภาพเดิมได้ด้วย (แต่ความจริงแล้วไม่สามารถแก้ไขได้ทุกไฟล์หรอก) ในส่วนของ CPAV จะมีเมนูสำหรับการทำงานอยู่ 2 โหมด คือ เมนูแบบรวบยอด (Express) ดังรูปที่ 5 และเมนูแบบเต็ม (Full) ดังรูปที่ 6 โดยในเมนูแบบเต็มจะมีข้อเลือกการทำงานได้มากกว่าการเปลี่ยนไปเปลี่ยนมาระหว่าง 2 เมนูจะต้องป้อนรหัสผ่านให้ถูกต้องก่อน โปรแกรม CPAV สามารถใช้งานด้วยเมาส์ได้ ซึ่งจะทำได้สะดวกยิ่งขึ้น




รูปที่ 5 เมนูของ CPAV ในโหมดของรวบยอด (Express)




รูปที่ 6 เมนูแบบเต็มของ CPAV ซึ่งมีข้อเลือกการทำงานได้มากกว่าในเมนูรวบยอด (Express)

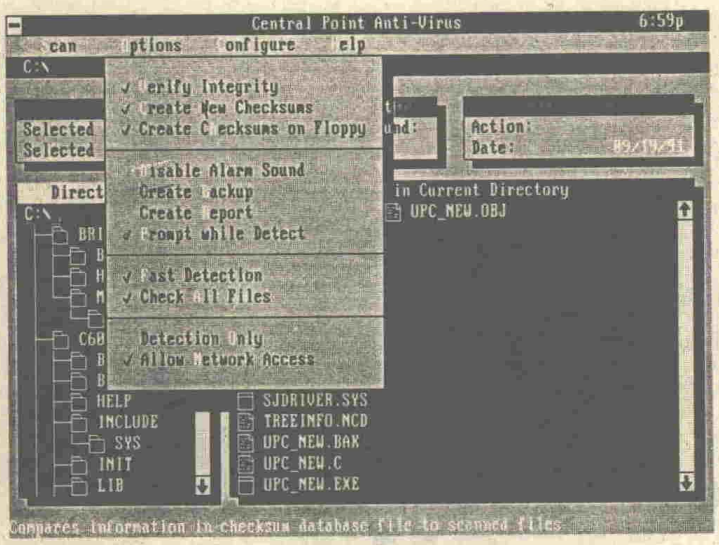
### - การสแกนหาไวรัส (SCAN)

การสแกนหาไวรัสของโปรแกรม CPAV จะเริ่มต้นจากการตรวจค้นจากหน่วยความจำก่อน จากนั้นจึงตรวจค้นจากไฟล์ในไดเรคทอรีที่เลือกเอาไว้ และระหว่างที่ผ่านแต่ละไดเรคทอรี CPAV ก็จะสร้างรายการไฟล์พร้อมทั้งค่าผลรวม (Checksum) ของแต่ละไฟล์เอาไว้ในไดเรคทอรีนั้น ๆ ด้วย เพื่อเอาไว้สำหรับเปรียบเทียบในการสแกนครั้งต่อไปเป็นการป้องกันการแพร่พันธุ์ของไวรัสที่ CPAV ไม่รู้จักได้

ถ้าหากการตรวจค้นหาข้อมูลทำงานช้าก็สามารถจะปรับแต่งการตรวจค้นได้จากเมนูของ Option ในรูปที่ 7

### - การฉีดวัคซีนรักษาตัวเอง

โปรแกรม CPAV สามารถจะฉีดวัคซีนเข้าไปในโปรแกรมแต่ละไฟล์บน




รูปที่ 7 เมนูใน Option สำหรับปรับแต่งวิธีการตรวจค้นหรือสแกนหาไวรัส ในหัวข้อเลือกสุดท้ายถ้าเครื่องอยู่ในระบบเน็ตเวอร์กก็สามารถเลือกให้ CPAV เข้าค้นข้อมูลในเน็ตเวอร์กได้

ดิสค์ให้มีคุณสมบัติป้องกันการแพร่กระจายไวรัสได้ด้วยตัวเอง เมื่อโปรแกรมที่ถูกฉีดวัคซีนถูกเรียกโปรแกรมวัคซีนจะตรวจสอบการเปลี่ยนแปลงของไฟล์โปรแกรม ซึ่งถ้ามีการเปลี่ยนแปลงเกิดขึ้นโปรแกรมดังกล่าวจะทำการรักษาตัวเองให้กลับสภาพเป็นอย่างเดิมได้

ตัวโปรแกรมวัคซีนมีขนาดน้อยกว่า 1 กิโลไบต์ โดยเกาะอยู่กับไฟล์โปรแกรมที่ถูกฉีด โปรแกรมวัคซีนจะไม่กินพื้นที่ในหน่วยความจำ การฉีดวัคซีนก็มีข้อจำกัด คือ

1. ไม่สามารถฉีดไฟล์ .EXE ที่มีการใช้งานโอเวอร์เลย์หรือกับโปรแกรมที่มีการเก็บข้อมูลเอาไว้ท้ายไฟล์ เช่น ข้อมูลสำหรับการช่วยดีบักโปรแกรม เป็นต้น

2. ไม่สามารถฉีดไฟล์ .EXE ที่มีข้อมูลในส่วนหัวไฟล์ (Header) ผิดได้

3. ไม่สามารถฉีดเข้าไฟล์ .EXE และ .COM ที่มีขนาดโปรแกรมน้อยกว่า 14 ไบต์ (ไม่รวมส่วนหัวในกรณี .EXE)

4. ไม่สามารถฉีดไฟล์ .COM ที่ใหญ่กว่า 63 กิโลไบต์

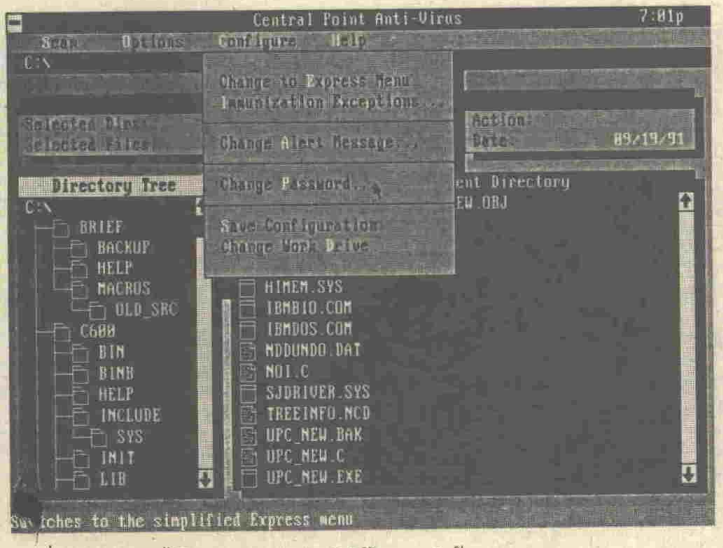
5. ไม่สามารถฉีดไฟล์ที่มีการตรวจสอบตัวเองได้

6. ไม่สามารถฉีดป้องกันไฟล์ของ Window และ OS/2 ได้

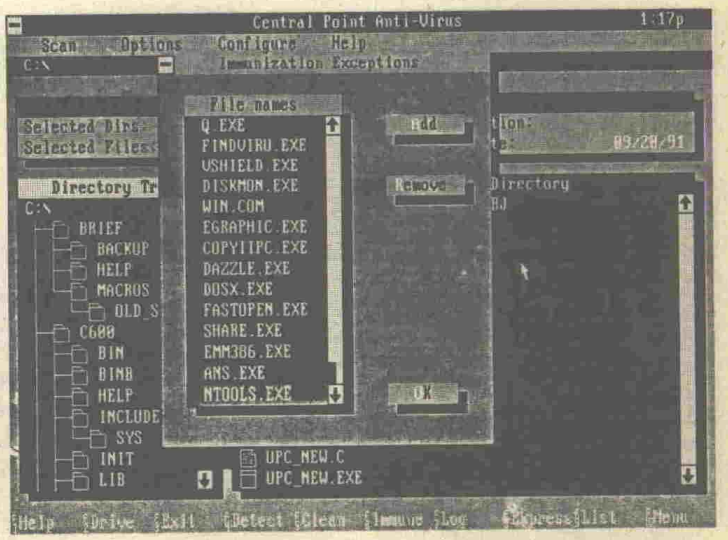
จากข้อจำกัดดังกล่าวจึงต้องมีการยกเว้นไฟล์บางไฟล์ ซึ่งสามารถทำได้โดยการเลือกเมนูจากเมนูในหัวข้อ Configure ตามรูปที่ 8 และรูปที่ 9

## - รายชื่อไวรัสที่ CPAV รู้จัก

ในตัว CPAV นั้นสามารถจะขอดูรายชื่อของไวรัสที่ CPAV สามารถ




รูปที่ 8 การติดตั้งโปรแกรม CPAV ทำได้ในเมนูหัวข้อ Configure




รูปที่ 9 การฉีดวัคซีนไม่สามารถทำได้กับทุก ๆ ไฟล์ ซึ่งมีการยกเว้นไฟล์บางไฟล์เสียก่อน

ตรวจค้นได้ (ดังรูปที่ 10) ซึ่งจะบอกชื่อไวรัส ประเภท และขนาดของไวรัสนั้น โดยสามารถสั่งพิมพ์ออกมาทางเครื่องพิมพ์ได้ด้วย

### - เพิ่มเติมรายการไวรัสพันธุ์ใหม่

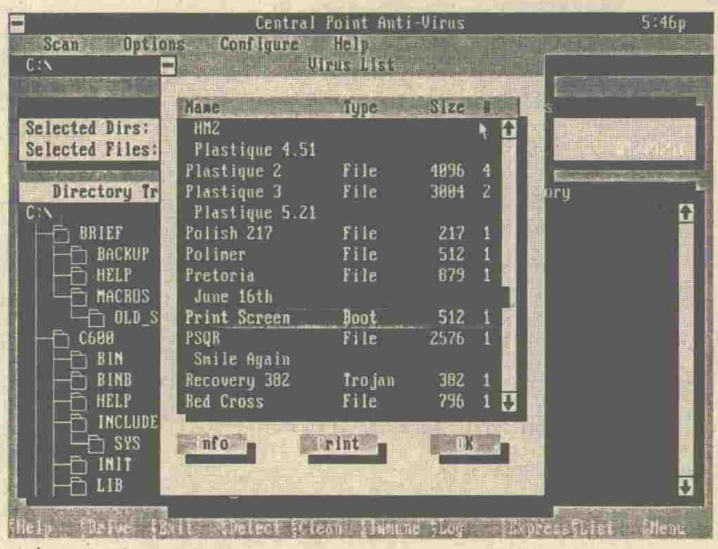
ใน CPAV นอกจากความสามารถในการตรวจค้นไวรัสคอมพิวเตอร์ที่รู้จักแล้ว ในกรณีของไวรัสพันธุ์ใหม่ ผู้ใช้ก็สามารถเพิ่มรายชื่อไวรัสให้กับ CPAV ได้ด้วย (ดังรูปที่ 11) แต่เท่าที่ผู้เขียนทดลองด้วยความพยายามอยู่หลายครั้งด้วยการหาลักษณะเฉพาะ (Signature) ของไวรัสเองแล้วป้อนเข้าไป แต่โปรแกรมไม่ยอมรับ ซึ่งอาจจะเป็นเพราะไม่ถูกรูปแบบก็ได้ อย่างไรก็ตาม ชื่อไวรัสพันธุ์ใหม่ในคู่มือแนะนำให้เอาจากบริษัท Central Point โดยตรง

### - การย้อนดูประวัติสภาพการตรวจค้น

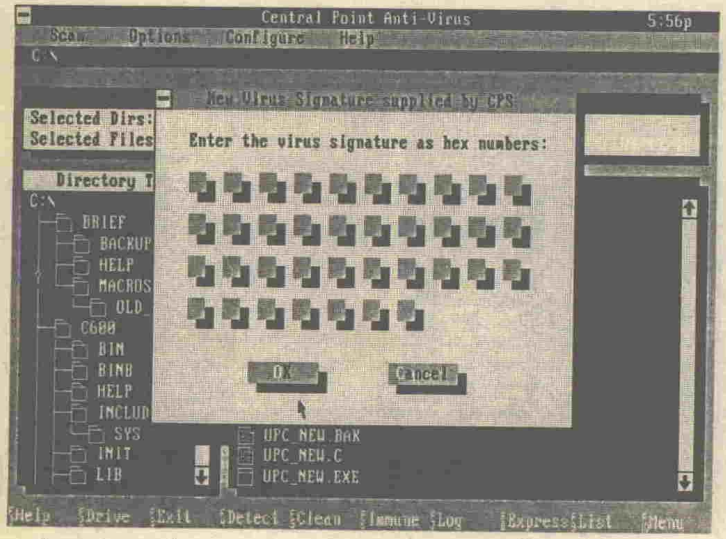
ในการสแกนตรวจค้นแต่ละตัวจะถูกบันทึกเอาไว้ ซึ่งสามารถจะนำกลับมาดูได้ (ดังรูปที่ 12)

## การติดตั้งโปรแกรม CPAV

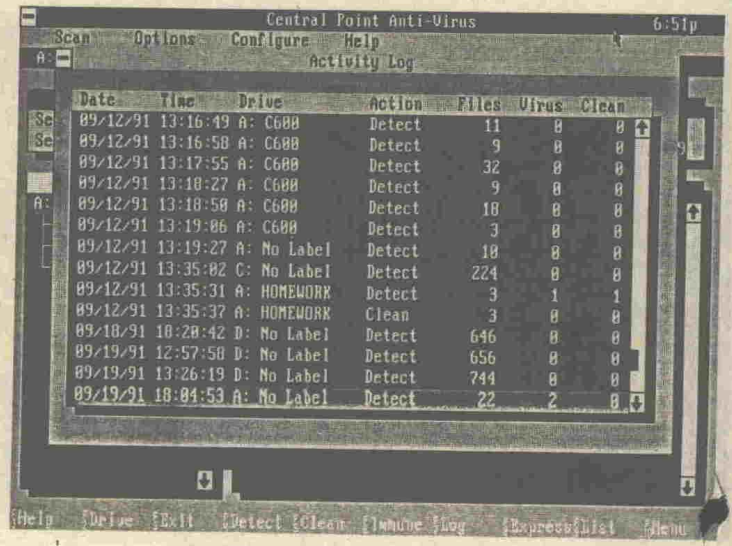
โปรแกรม Install สำหรับติดตั้งจะมีข้อเลือกดังรูปที่ 2 ซึ่ง Install สามารถ



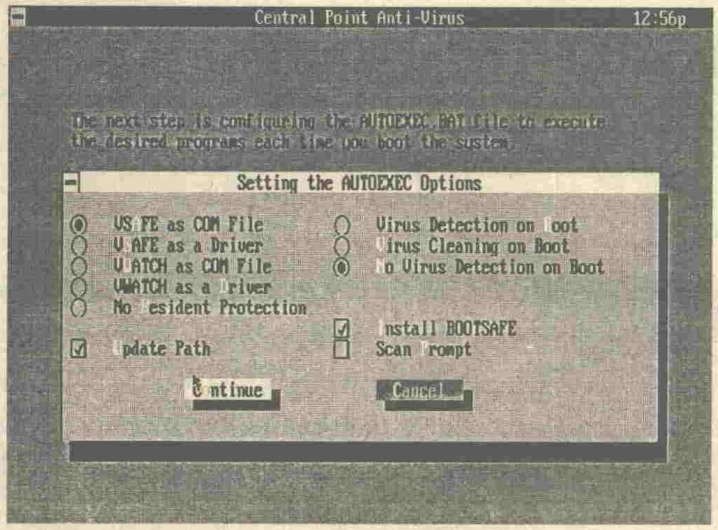

รูปที่ 10 รายชื่อไวรัสที่ CPAV สามารถสแกนตรวจได้




รูปที่ 11 สามารถเพิ่มรายการไวรัสพันธุ์ใหม่ให้กับโปรแกรม CPAV ได้เลย




รูปที่ 12 การสแกนตรวจค้นแต่ละครั้งจะมีการบันทึกเอาไว้เสมอ




รูปที่ 13 การเลือกชุดโปรแกรม CPAV ขณะติดตั้ง

เรียกใช้งานเมื่อไรก็ได้ ในหัวข้อแรกของเมนูคือ Install จะมีการตรวจสอบหาไวรัสในหน่วยความจำและในแต่ละไดเรคทอรี ผู้ติดตั้งสามารถเลือกชุดโปรแกรมที่จะติดตั้งได้ ดังรูปที่ 13 สำหรับการติดตั้งครั้งแรกในคู่มือแนะนำให้ทำการสร้างแผ่นดิสก์ฉุกเฉินเอาไว้เพื่อเก็บรักษาและนำมาใช้เมื่อฮาร์ดดิสก์มีอาการผิดปกติหรือถูกทำลายในพื้นที่ของตารางแบ่งส่วน นอกจากนั้นผู้ใช้สามารถปรับแต่งสีสรรของโปรแกรมได้ตามชอบใจ ในหัวข้อของ Interface Option

## CPAV กับวินโดวส์

ในกรณีที่จะใช้ CPAV ร่วมกับไวรัสนั้นในคู่มือบอกไว้ว่า โปรแกรม VSafe ซึ่งเป็นโปรแกรมเรสซิเดนต์นั้น ถ้าตรวจพบอาการผิดปกติจะมีแต่เสียงร้องเตือนเท่านั้น โดยจะไม่แสดงข้อมูลอะไรออกมา ซึ่งผู้ใช้ต้องสังเกตและคอยฟังเสียงเอา และถ้าต้องการใช้ CPAV สแกนตรวจค้นเมื่ออยู่บนวินโดวส์ให้เรียก CPAV โดยใส่ /NF ตามหลังเพื่อยกเลิกโปรแกรม

## สรุป

ผู้เขียนคิดว่าข้อมูลต่าง ๆ ของโปรแกรมต่อต้านไวรัสคงจะช่วยให้ผู้อ่านสามารถเรียกซื้อโปรแกรมได้อย่างรอบคอบขึ้น ตราบใดที่ไวรัสยังเกิดขึ้นใหม่ตลอดเวลา โปรแกรมต่อต้านไวรัสก็ยิ่งจะมีความสำคัญมากขึ้นตามลำดับ